

EDOK - Application for Search Warrant (Revised 5/13)

United States District Court

EASTERN DISTRICT OF OKLAHOMA

In the matter of the search of one (1) Samsung Galaxy cellular telephone, model #SM-G970U, IMEI #354774100192626, currently located at Sequoyah County Sheriff's Office, Sallisaw, Oklahoma

Case No. 23-MJ-238-DES

APPLICATION FOR SEARCH WARRANT

I, Brett J. Collins, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the EASTERN District of OKLAHOMA (identify the person or describe property to be searched and give its location):

SEE ATTACHMENT "A"

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

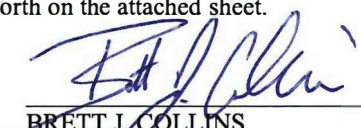
SEE ATTACHMENT "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 18 United States Code, Sections 2241(c), 2423(b), 2251(a), 2252(a)(1), and/or 2252(a)(4)(B), and the application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


BRETT J. COLLINS
 Special Agent
 Federal Bureau of Investigation

Sworn to: _____

Date: 9/20/2023

City and state: Muskogee, Oklahoma




 Judge's signature
D. EDWARD SNOW
UNITED STATES MAGISTRATE JUDGE
 Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Brett J. Collins, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been employed as a Special Agent (SA) with the Federal Bureau of Investigation (FBI) since 2017 and am currently assigned to the Oklahoma City Division, Fort Smith Resident Agency, of the FBI. I am an investigative officer, or law enforcement officer, of the United States of America within the meaning of 18 U.S.C. § 2510(7) and Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure, that is, an officer of the United States who is empowered by law to conduct investigation of, and make arrests for, offenses enumerated in Title 18 of the United States Code. During my time as an SA for the FBI, I have conducted and participated in a wide variety of investigations, including Indian Country crimes, as defined in 18 U.S.C. §§ 1151 and 1153, including violent crimes and child abuse crimes.

3. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the

application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2241(c), 2423(b), 2251(a), 2252(a)(1), and/or 2252(a)(4)(B) (“the Subject Offenses”), have been committed by MICHAEL WAYNE GREEN. There is also probable cause to search the items described in Attachment A for evidence, instrumentalities, and/or fruits of these crimes further described in Attachment B.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is a Samsung Galaxy cellular telephone, model #SM-G970U, IMEI #354774100192626, Serial #R58M224YK7A, hereinafter the “**Device**.” The **Device** is currently located at the Sequoyah County Sheriff’s Office (“SCSO”), 119 S. Oak Street, Sallisaw, Oklahoma. The **Device** will be taken into FBI custody after I swear to the facts in this affidavit.

6. The applied-for warrant would authorize the forensic examination of the **Device** for the purpose of identifying electronically stored data particularly described in Attachment B.

BACKGROUND

7. The **Device** is currently in the lawful possession of SCSO. SCSO investigators obtained a state search warrant for the **Device** in the District Court of Sequoyah County (Case #SW-23-30) on or about June 6, 2023. On or about June 7, 2023, a Sallisaw Police Department (“SPD”) detective performed a full file system extraction on the **Device**. The **Device** is currently located in the evidence control room at SCSO. In my training and experience, I know that the **Device** has been stored in a manner in which its contents are, to the extent material to this

investigation, in substantially the same state as they were when the **Device** first came into SCSO's possession on or about June 5, 2023.

PROBABLE CAUSE

8. On August 6, 2022, L.H. reported that her 8-year-old daughter, E.H., disclosed that E.H. had been sexually molested by her step-grandfather, Michael W. Green ("GREEN"), in Sallisaw, Sequoyah County, Oklahoma, while Green was visiting the family from on or about July 21, 2022 through August 5, 2022. GREEN during that period resided in Irving, Texas. In addition, on or about August 16, 2022, J.H., E.H.'s father and GREEN's stepson, stated he was advised by L.H. that one of his children, later identified as E.H., disclosed observing photos of children on GREEN's cellular telephone ("cell phone").

9. On or about August 18, 2022, E.H. was forensically interviewed. During the interview, E.H. disclosed that GREEN, on more than one occasion, took sexually explicit photos of her with his cell phone while E.H. was in GREEN's truck, which was parked in the driveway at L.H. and J.H.'s residence in Sallisaw. Specifically, E.H. stated that GREEN instructed her to pull her pants down and took photos of her vagina with his cell phone while she was sitting in the front seat of his truck. E.H. further disclosed that GREEN also took photos of her vagina and buttocks in the back seat of GREEN's truck. E.H. stated that she had also observed pictures of young girls on GREEN's cell phone, which GREEN told her were from the internet.

10. Based on SCSO's investigation, an arrest warrant was issued for GREEN by the Sequoyah County District Attorney's Office. Subsequently, on or about August 18, 2022, GREEN was arrested at his residence in Irving, Texas by members of the Irving Police Department ("IPD"). GREEN was in possession of the **Device** at the time of his arrest. The **Device** was seized and submitted to evidence by IPD.

11. On or about June 5, 2023, the SCSO received the **Device** from IPD via FedEx. As described above, SCSO investigators obtained a state search warrant for the **Device** on June 6, 2023. During my review of the contents of the **Device**, I observed location data that confirmed GREEN's presence in the Eastern District of Oklahoma in late July and early August 2022. I located multiple pornographic images and videos of E.H., corroborating the disclosures she made during her forensic interview. Specifically, there were multiple images of E.H. posed in a way, and the frame of the camera was such, that E.H.'s vagina and anus were the focal points of the images and videos. Metadata associated with the images and videos of E.H. indicated that they were captured using the **Device** between on or about July 23, 2022 and on or about July 26, 2022, during which time GREEN was in the Eastern District of Oklahoma. In addition, I located in excess of 1,000 images and 60 videos containing child sexual abuse material ("CSAM") on the **Device**.

12. On or about September 13, 2023, in the Eastern District of Oklahoma, a federal grand jury returned an indictment charging GREEN with Aggravated Sexual Abuse, in violation of 18 U.S.C. §§ 2241(c) and 2246(2), Travel with Intent to Engage in Illicit Sexual Conduct, in violation of 18 U.S.C. §§ 2423(b) and 2423(e), Sexual Exploitation of a Child/Use of a Child to Produce a Visual Depiction, in violation of 18 U.S.C. §§ 2251(a) and 2251(e), Transportation of Certain Material Involving the Sexual Exploitation of a Minor, in violation of 18 U.S.C. §§ 2252(a)(1) and 2252(b)(1), and Possession of Certain Material Involving the Sexual Exploitation of a Minor, in violation of 18 U.S.C. §§ 2252(a)(4)(B) and 2252(b)(2). An arrest warrant for GREEN was subsequently issued for these charges. GREEN is currently in federal custody.

13. I seek this additional warrant out of an abundance of caution to be certain that an examination of the **Device** will comply with the Fourth Amendment and other applicable laws. A new examination of the **Device** could retrieve artifacts not previously obtained. Based on my

conversations with FBI personnel trained in digital forensics, I am aware that the forensic support for evidence obtained from cell phones is constantly evolving. Manufacturers of cellular devices frequently change and update their operating system software for a multitude of reasons. This will prompt the digital forensic tool companies to update their software in order to search, extract and interpret the constantly changing data more effectively than only months before. A new examination of the **Device** by FBI's Computer Analysis Response Team ("CART") will most likely provide access to more data than was available at the time of the previous extraction.

TECHNICAL TERMS

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading

information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved

in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function

as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- g. **Pager:** A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.
- h. **IP Address:** An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- i. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

15. Based on my training, experience, and research, I know that the **Device** has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

CHARACTERISTICS COMMON IN INDIVIDUALS WHO EXHIBIT A SEXUAL INTEREST IN CHILDREN AND INDIVIDUALS WHO DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

16. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

17. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

18. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

19. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years.

20. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly.¹ Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

21. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences.

22. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings, or engage in contact sex offenses with children. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child pornographic or child erotica images, videos or other recordings. Studies have shown there is a high cooccurrence between those who traffic in child pornography

¹ The Tenth Circuit recognized that "collectors of child pornography are likely to 'hoard' the materials." *United States v. Potts*, 586 F.3d 823, 828-29 (10th Cir. 2009).

and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared.

23. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.²

24. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

25. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

² See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)); *United States v. Frechette*, 583 F.3d 374, 379 (6th Cir. 2009) ("Unlike cases involving narcotics that are bought, sold, or used, digital images of child pornography can be easily duplicated and kept indefinitely even if they are sold or traded. In short, images of child pornography can have an infinite life span.").

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

26. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

27. Computers, smartphones and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers and smartphones basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

28. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

29. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers and smartphones and tablets around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

30. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives,

which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also almost always carried on an individual's person (or within their immediate dominion and control) and can additionally store media.

31. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

32. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases.

33. As is the case with most digital technology, communications by way of computer or smartphone can be saved or stored on the computer or smartphone used for these purposes. Storing this information can be intentional (i.e., by saving an e-mail as a file on the computer or smartphone, or saving the location of one's favorite websites in, for example, “bookmarked” files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer or

smartphone user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

34. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **Device** in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, such as a cellular phone, smartphone, or tablet. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

35. I submit that there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

36. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

37. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

38. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

39. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

40. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how the **Device** was used, the purpose of the use, who used the **Device**, and when. There is probable cause to believe that this forensic electronic evidence will be on the **Device** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage

media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified;

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that logs the following: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic

storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement);

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when;
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance

the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant;

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent;
- f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

41. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be

stored on a variety of computer systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, smartphones, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that:

- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;
- b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

- c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of a premises; and
- d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

42. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might

expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

43. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

44. I know that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities, including possession, receipt, and distribution of child pornography. These photos are sometimes stored in their cellular phones and often are transmitted or sent from one electronic media device to another. I also know that cellular phones may also contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are often used by two or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

45. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications (telephone calls and FaceTime type communications) as well as applications like “Instagram” and “Facebook.” Additionally, individuals utilize their cellular devices to take pictures, keep notes, as a GPS (global positioning System) device, and even to conduct illicit or illegal activity. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through

the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual. This data includes contacts used to conduct illegal activities to include possession, receipt, and distribution of child pornography.

46. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information. This information may be contained on the cellular telephone.

47. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **Device** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Device** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to possess, receive, and distribute child pornography, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of

how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

48. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **Device** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the **Device** to human inspection in order to determine whether it is evidence described by the warrant.

49. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

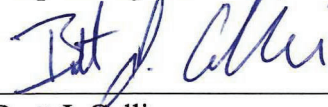
50. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crimes under investigation, including but not limited to undertaking a cursory inspection of all information within the **Device**. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications.

Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

CONCLUSION

51. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the **Device** described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Brett J. Collins
Special Agent
Federal Bureau of Investigation

Sworn to me on September 20, 2023:



UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a Samsung Galaxy cellular telephone, model #SM-G970U, IMEI #354774100192626, Serial #R58M224YK7A, hereinafter the “**Device**.” The **Device** is currently located at the Sequoyah County Sheriff’s Office (“SCSO”), 119 S. Oak Street, Sallisaw, Oklahoma.

This warrant authorizes the forensic examination of the **Device** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the **Device** described in Attachment A that relate to violations of 18 U.S.C. §§ 2241(c), 2423(b), 2251(a), 2252(a)(1), and/or 2252(a)(4)(B) (the “Subject Offenses”), and involve Michael Wayne GREEN, including:

a. Images/videos/gifs of child pornography or child erotica; files containing images/videos/gifs; and data of any type relating to the sexual exploitation of minors or a sexual interest in children, material related to the possession thereof, and data of any type related to any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting such visual depiction of such conduct, in any form wherever it may be stored or found, including, but not limited to:

i. Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG) of child pornography; files relating to the distribution, receipt, or possession of child pornography, or information pertaining to an interest in child pornography;

ii. Files in any form containing the visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors; and

iii. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit

conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors.

2. Information, correspondence, records, documents or other materials pertaining to the Subject Offenses, or pertaining to the sexual exploitation of minors or a sexual interest in children, that were transmitted or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

- a. Correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;
- b. Any and all electronic and/or digital records and/or documents pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors;
- c. Any and all electronic and/or digital records and/or documents including any and all address books, names, and lists of names and addresses of minors visually

depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors;

- d. Any and all records of Internet usage including usernames and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums;
- e. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;
- f. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and
- g. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software.

3. Records or other items which evidence ownership, use, or control of the **Device** described in Attachment A, including:

- a. Evidence of user attribution showing who used or owned the **Device** at the time the things described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history;
- b. Records and information relating to geolocation and travel in furtherance of the Subject Offenses;

- c. Records relating to communication with others as to the Subject Offenses; including incoming and outgoing voice messages; text messages; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, including those derived from Skype, Line 2, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;
 - d. Threatening communications related to the Subject Offenses;
 - e. Records relating to documentation or memorialization of the Subject Offenses, including voice memos, photographs, videos, and other audio and video media, and all EXIF information and metadata attached thereto including device information, geotagging information, and information of the relevant dates to the media;
 - f. Records relating to the planning and execution of the Subject Offenses, including Internet activity, including firewall logs, caches, browser history, and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;
 - g. Application data relating to the Subject Offenses; and/or
 - h. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the Subject Offenses;
4. Any and all records of Internet usage including usernames and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may

include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums.

5. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

6. Any and all information, correspondence (including emails), records, documents and/or other materials related to contacts, in whatever form, with minors involving the production, possession and/or distribution of child pornography and the attempt or act of seducing, enticing, coercing, or persuading a minor to engage in sexual acts.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage.

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and

instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.